UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/087,974	03/04/2002	Ronald Leo Christiaan Koymans	PHNL 010153	6966

24737	7590	03/16/2006

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER
DAFTUAR, SAKET K

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 03/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

MAILED

MAR 1 6 2006

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/087,974
Filing Date: March 04, 2002
Appellant(s): KOYMANS ET AL.

Dicran Halajian, Registration number 39,703
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 02/08/2006.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix A

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Appendix B: Evidence Relied Upon

B1.   Method and Apparatus for Protecting Information by Rabin et al,

U.S. Patent Number 6,697,948 B1, issued on February 24th, 2004, but filed

on May 5th, 1999 (hereinafter Rabin).

B2.   "Interoperability", Answers.com,

http://www.answers.com/topic/interoperability?method=22, pages 1-4.

(9) Grounds of Rejection

Claims 1- 14 are rejected under 35 U.S.C. 102(e) as being anticipated by

Rabin et al. U.S. Patent Number 6,697,948 B1 (hereinafter Rabin).

As per claim 1 Rabin discloses loading a new system component into a

system with a computer [Software instances, see column 3 lines 47-49]; in

response to said loading, sending information about said system component and

a configuration of the system with a to an acceptance server via a remote

communication network [Tag server accepting instances of software, see column

3 lines 47-50]; verifying with said acceptance server whether the system with a

computer including the system component and configured according to

information about the configuration meets a criterion of interoperability

[Supervisory programs verifies the authenticity of the tag, see column 3 lines 55-

59]; sending an acceptance signal from the acceptance server to the system with

a computer via the remote communication network [hash function values and

unique identifier determine if the tag is authentic or not, see column 4 lines 10-

16]; qualifying operation of the system with a computer including the system component dependent on the acceptance signal [Supervisory programs verify the hash function value and identifier to satisfy a tag associated with software instances, see column 4 lines 15-20].

As per claim 2, Rabin discloses sending information that determines a computer program for controlling a controllable apparatus from the controllable apparatus to the system with a computer, when the controllable apparatus is coupled to the system with a computer via a local communication network [Software instances having unique tag, see column 7 lines 53-62]; said system component being the computer program, the acceptance server being directed at verifying whether the computer program will execute in the configuration according to the criterion of interoperability[The software instances associated with a tag satisfy a same location fingerprint check, see column 4 lines 17-20; examiner considers software instances performing fingerprint check with a computer program (supervisory program)]; control of an operation of the controllable apparatus by the system with a computer with the computer program being qualified according to the acceptance signal[User device includes supervisory program, see column 3 lines 55-56].

As per claim 3, Rabin discloses a new system component into the system [Software instances, see column 3 lines 47-49]; an acceptance server [Tag

server accepting instances of software, see column 3 lines 47-50]; a remote

communication network [see column 27, lines 7-14]; an apparatus coupled to the

acceptance server via the remote communication network, the apparatus being

arranged to send information about said system component and a configuration

of the system with a computer to the acceptance server via the remote

communication network, in response to said loading[user device downloading

software instances electronically and installed from software vendor via

communication network, see column 27 lines 25-30]; said acceptance server

being arranged to verify whether the system with a computer including the

system component and configured according to information about the

configuration meets a criterion of interoperability and to send an acceptance

signal to the system with a computer via the remote communication network[The

tag server, coupled to communication network to creates or generates a tag for

each instances of software, see column 27 lines 30-32]; the apparatus being

arranged to qualify operation of the system with a computer including the system

component dependent on the acceptance signal[Each tag has a unique identifier

of the supervisory program, see column 4 lines 5-9].

As per claim 4, Rabin discloses the computer [see column 2 lines 55-56];

an input for receiving a computer program for execution by the computer [user

device includes input port that receives an instance of software, see column 8

lines 13-17]; an communication interface for communication to a remote

acceptance server, the apparatus being arranged to send information about the

computer program and a configuration of apparatus to the acceptance server and

to receive an acceptance server in return to said information, the apparatus being

arranged to qualify execution of the computer program by the computer

according to the acceptance signal [see column 39, lines 1-4, examiner

considers interconnection mechanism coupled to the user device and securely

transmit tag information to tag server].

As per claim 5, Rabin discloses a connection [Interconnection mechanism,

see column 8 lines 50-52] for connection to a controllable apparatus, the

connection comprising said input for receiving the computer program, the

computer program being a program for controlling the controllable apparatus via

the connection, the apparatus qualifying control of the controllable apparatus

according to the acceptance signal [user device includes input port that receives

an instance of software, see column 8 lines 13-17];

As per claim 6, Rabin discloses the information about the configuration

identifying the type of an apparatus, said criterion including a sub-criterion for the

compatibility of the apparatus, as identified by the information about the

configuration, and the computer program [see column 54 lines 1-11, two devices

having same tag performs a call-up, tag is copied from another, Only one of the

device will accept the continuation because the header tag table matches only one ID tag].

As per claim 7, Rabin discloses the computer program being arranged to execute selectable ones of a plurality of functions, the acceptance signal comprising an identification of the acceptability of respective ones of the functions, said qualifying being selective for the respective functions [see column 3 lines 47-53, each tag uniquely identified the instances of software].

As per claim 8, Rabin discloses that said qualifying comprises disabling execution of a part or whole of computer program, as far as identified as unacceptable by the acceptance signal [supervisory program rejects the instance of software if the tag associated with the software is not authentic, see column 3 lines 63-65].

As per claim 9, Rabin discloses said qualifying comprises generating a warning signal to a user about the computer program or parts thereof when a user attempts to cause operation of computer program or the parts thereof and/or generating the warning signal upon any first user action after reception of the acceptance signal [tag generating hash function value and digital signature for supervisory program to verify and determine if the tag is authentic, see column 4 lines 1-15].

As per claim 10, Rabin discloses the apparatus being arranged to execute enable unqualified execution at least part of the computer program until the apparatus has received the acceptance signal received from the acceptance server [for untagged software, the verification program periodically executes a call-up procedures to receive; if the verification program detects a match, a specific punitive action to be performed, see column 17 lines 18-30].

As per claim 11, Rabin discloses providing an acceptance server coupled to a communication network [The tag server, coupled to communication network to creates or generates a tag for each instances of software, see column 27 lines 30-32]; receiving information with the server about a configuration of the system with a computer and a new system component of that system with a computer via the communication network [user device downloading software instances electronically and installed from software vendor via communication network, see column 27 lines 25-30]; checking with the server whether the system component and configured according to information about the configuration meets a criterion of interoperability[see column 3 lines 47-53, each tag uniquely identified the instances of software]; sending an acceptance signal back from the server to a source of said information, the acceptance signal signaling whether said criterion of interoperability is met[The software instances associated with a tag satisfy a same location fingerprint check, see column 4 lines 17-20; examiner considers

software instances performing fingerprint check with a computer program (supervisory program)].

As per claim 12, Rabin discloses the server is selectively reachable through the communication network using [see column 27, lines 7-14] a network address, the network address being specific to a predetermined type of apparatus, or family of types of apparatuses, the criterion being specialized to said family [see column 44, line 2-6].

As per claim 13, Rabin discloses the new component is a computer program, the information comprising at least part of a code of said computer program, the method comprising analyzing the executable code with the server to determine whether its effect meets the criterion when executed by the system with a computer [see column 13 lines 37-47 and column 32 lines 14-17].

As per claim 14, Rabin discloses the computer program is arranged to handle selectable ones of a set of events, the server determining handling which of the events meets said criterion, the acceptance signal particularizing which of the events are acceptable [see column 54 lines 1-11, two devices having same tag performs a call-up, tag is copied from another, Only one of the device will accept the continuation because the header tag table matches only one ID tag].

(10) Response to Argument

As per appellants' arguments filed on August 25th, 2005, the applicant's argue in substance that:

a.   Rabin fails to determine "criterion of interoperability" between a computer system and a new system loaded into the computer (see appeal brief, pages 9 and 10).

In response to applicant amended argument a), Rabin teaches determining criterion of interoperability between a computer system and a new system loaded into the computer [As admitted by appellants criterion of interoperability is based upon nature of available apparatuses and version of software (specification, page 10). Examiner interprets the term interoperability (software version) is used to describe the capability of different programs to share or exchange data (See Appendix B (B2)). Rabin discloses the capability of supervising program (see column 60, lines 30-42) and verifying program (see column 5, lines 9-28). Rabin discloses the supervising program that updates the hash of the data tag table after each update. Rabin also discloses verifying the hash function before updating the tag table and the supervising program takes punitive action if it fails. In this manner Rabin uses the current invention to detect if device and software is opera table (share or exchange data) and hence, maintains the criterion of interoperability. Rabin also discloses a verification program that examines each tag received from the user device against the tagged software database to ensure that the tags are in compliance with at least one usage supervision policy.

In addition Rabin also discloses that the supervision program on the user device receives and verifies the continuation message for authenticity and if authentic, performs the action to follow indicated in the continuation message and hence, determining access to software on user devices by controlling tag usage status discloses meeting criterion of interoperability to describe the capability of software programs to exchange data].

b. Appellant's argues that tampering is not related to interoperability. A device of software can be tampered and still meet criterion of interoperability and the intent of Rabin is to detect and prevent tampering and piracy (see brief page 9).

In response to appellant's arguments b), tampering is not related to interoperability and a device of software can be tampered and still meet the criterion of interoperability is not persuasive. Examiner agrees that Rabin is concerned with preventing tampering so as to prevent unauthorized use or using an illegal copy of the software program and the intent of Rabin is to detect and prevent tampering and piracy. In addition, examiner considers the term interoperability is used to describe the capability of different programs to exchange data via a common set of business procedures, and to read or write the same file formats (emphasis added) and use the same protocol [See Appendix B (B2)]. In embodiment, Rabin has presented a mechanism to detect, control and supervise usage of fingerprinting program (an instance of software program). Rabin further discloses the operation of fingerprinting and its software
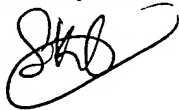
operation with same specific legitimate software [same file format] for verification and authenticity. When any of these, periodic, checks fail, examiner interprets the software program performs a punitive action to stop exchanging and sharing data (see column 60, lines 7-67).

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

SKD

Conferees: